CLAIMS

What is claimed is:

1. A method for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transfer protocol, the method comprising the computer-implemented steps of:

selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads;

based on the subset and the secret integer, generating encrypted data that is impractical for a device other than the client and the server to decrypt; and

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data and clue information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

2. A method as recited in Claim 1, wherein the unencrypted transfer protocol is Hypertext Transfer Protocol (HTTP).

3. A method as recited in Claim 1, said step of determining a secret integer that is unique for the subset further comprising the steps of:

generating a first integer using a random number generator;

determining a shared secret key to be shared with the receiving device based on the first integer and a first public key associated with the receiving device; and

selecting the secret integer based on the shared secret key.

4. A method as recited in Claim 3, said step of sending the information to determine the secret integer further comprising the steps of:

determining a second public key associated with the sending device based on the first integer; and

including the second public key in the information to determine the secret integer.

5. A method as recited in Claim 3, said step of sending the information to determine the secret integer further comprising the steps of:

determining a plurality of second public keys associated with the sending device based on the first integer, wherein each of the second public keys is associated with one of a plurality of subsets from the set of data; and

including the plurality of second public keys in the information to determine the secret integer.

6. A method as recited in Claim 3, said step of setting the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer.

7. A method as recited in Claim 3, said step of generating encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the subset and the secret integer to generate the encrypted data.

8. A method as recited in Claim 1, wherein:

said step of determining the secret integer further comprises the step of applying a particular hash function a plurality of times to a shared secret key shared with the receiving device; and

said step of sending the information to determine the secret integer further comprises the step of storing, as part of the clue information, data that indicates a number of times the particular hash function has been applied.

9. A method as recited in Claim 8, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information;

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated in the information; and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer.

10. A method as recited in Claim 8, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information;

determining a second integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the first integer; and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer.

11. A method as recited in Claim 8, further comprising, before said step of determining the secret integer, performing the steps of:

determining the shared secret key based on a particular communication between the client and the server; and

storing the shared secret key in a secure data structure.

12. A method as recited in Claim 1, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server.

13. A method as recited in Claim 1, wherein the secret integer has a number of bits that varies in accordance with lengths of payloads that are communicated during a communication session between the client and the server.

14. A method for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload associated with the transport protocol, the method comprising the computer-implemented steps of:

receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and clue information to determine, only at the client and the server, a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads;

determining the secret integer based, at least in part, on the clue information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server.

15. A method as recited in Claim 14, wherein the unencrypted transfer protocol is the Hypertext Transfer Protocol (HTTP).

16. A method as recited in Claim 14, said step of determining the secret integer further comprising the steps of:

based on the clue information, determining a shared secret key shared with the sending device; and

generating the secret integer based on the shared secret key.

17. A method as recited in Claim 16, said step of generating the secret integer further comprising the step of applying a particular hash function to the shared secret key to generate the secret integer.

18. A method as recited in Claim 14, wherein:

the method further comprises the steps of

determining a shared secret key based on a particular communication between the client and the server, and

storing the shared secret key in a secure data structure; and

the clue information indicates a number of times a particular hash function is applied to the shared secret key in generating the secret integer.

19. A method as recited in Claim 18, said step of determining the secret integer further comprising the step of causing the particular hash function to be applied the number of times indicated by the clue information to the shared secret key:

20. A method as recited in Claim 19, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated by the clue information;

determining a second integer formed after the particular hash function is applied fewer times than the number of times indicated by the clue information; and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer.

21. A method as recited in Claim 19, said step of determining the secret integer further comprising the steps of:

determining a first integer formed after the particular hash function is applied the number of times indicated in the information;

determining a second integer formed after a second hash function is applied for the number of times indicated in the information, wherein the second hash function is different from the particular hash function that is used to determine the first integer; and

performing an exclusive or (XOR) operation between corresponding bits of the first integer and the second integer.

22. A method as recited in Claim 14, said step of decrypting the encrypted data further comprising the step of performing an exclusive or (XOR) operation between corresponding bits of the encrypted data and the secret integer to generate the subset of data.

23. A method as recited in Claim 14, wherein the secret integer has a particular number of bits fixed for all subsets in all payloads communicated during a communication session between the client and the server.

24. A computer-readable medium carrying one or more sequences of instructions for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads;

based on the subset and the secret integer, generating encrypted data that is practically unintelligible to a device other than the client and the server; and

sending, from a sending device of the client and the server to a receiving device of the client and the server, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

25. A computer-readable medium carrying one or more sequences of instructions for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and information to determine, only at the client and the server, a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads;

determining the secret integer based, at least in part, on the information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server.

26. An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

means for selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

means for determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads;

means for generating, based on the subset and the secret integer, encrypted data that is practically unintelligible to a device other than the client and the server; and

means for sending to a receiving device of the client and the server, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

27. An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

means for receiving, at a receiving device of the client and the server from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and information to determine, only at the client and the server, a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads;

means for determining the secret integer based, at least in part, on the information; and

means for decrypting the encrypted data, based on the secret integer, to generate a subset of data to be communicated between client and server.

28. An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

a network interface that is coupled to the data network for sending one or more packet flows thereto;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

selecting a subset from a set of data to be communicated between the client and the server in a particular payload of the unencrypted transfer protocol;

determining a secret integer that is unique for the subset among a plurality of subsets in a plurality of payloads;

based on the subset and the secret integer, generating encrypted data that is practically unintelligible to a device other than the client and the server; and

sending, to a receiving device of the client and the server, in the particular payload, the encrypted data and information to determine, only at the client and the server, the secret integer for decrypting the encrypted data.

29. An apparatus for securing data in communications between a client and server using an unencrypted transfer protocol that does not encrypt a payload defined by the transport protocol, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving, from a sending device of the client and the server, in a particular payload of the unencrypted transfer protocol, encrypted data and information to determine, only at the client and the server, a secret integer unique for the encrypted data in the particular payload among a plurality of subsets in a plurality of payloads;

determining the secret integer based, at least in part, on the information; and

based on the secret integer, decrypting the encrypted data to generate a subset of data to be communicated between client and server.